REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-01-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
07-2003	Journal Article	

4. TITLE AND SUBTITLE
Cyclic Code Shift Keying: A Low Probability of Intercept Communication Technique

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHORS
George M. Dillard[1]
Michael Reuter[2]
James Zeidler, Brandon Zeidler[3]

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

1. SSC San Diego
53560 Hull Street
San Diego, CA 92152

2. Motorola Automotive and Electronic Systems Group
21440 Lake Cook Road
Deer Park, IL 60010

3. University of California at San Diego, Mail Code 0407
9500 Gilman Drive
La Jolla, CA 92093-0407

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
A low probability of intercept (LPI), or low probability of detection (LPD) communication technique known as cyclic code shift keying (CCSK) is described. We discuss the basic concepts of CCSK and describe a system based on the use of random or pseudorandom codes for biphase modulation. We use simulation to show that the bit error rate (BER) for CCSK can be closely estimated by using existing equations that apply to M –ary orthogonal signaling (MOS). Also, we show that significantly fewer computations are required for CCSK than for MOS when the number of bits per symbol is the same. We show that using biphase modulation results in waveforms that have a large time-bandwidth product and very low input signal-to-noise ratio (SNR) and thus inherently have an LPI by a radiometer. We evaluate detection by a radiometer and show that LPI can be achieved by using codes of lengths great than about 2^{12} (i.e., by transmitting more than about 12 bits per symbol). Results illustrate the effect that the CCSK symbol length and error probability, and the radiometer integration time and probablility of false alarm (PFA), have on detection by a radiometer. We describe a variation of CCSK called truncated CCSK (TCCSK). In this system, the code on length 2^k is cyclically shifted, then truncated and transmitted. Although shortened, the trucated code still represents k bits of information, thus leading to an increased data rate. We evaluate radiometer detection of TCCSK and it is shown that the probability of detection is increased compared with the detection of CCSK.

Published in *IEEE Transactions on Aerospace and Electronic Systems*. Vol. 39, No. 3, pp. 786–798, July 2003.

15. SUBJECT TERMS
Cyclic code shift keying (CCSK)
low probability of detection (LPD)
low probability of intercept (LPI)
radiometry

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			James Zeidler, Email: zeidler@ece.ucsd.edu
U	U	U	UU	12	19B. TELEPHONE NUMBER *(Include area code)* (858) 534-5369

Cyclic Code Shift Keying: A Low Probability of Intercept Communication Technique

GEORGE M. DILLARD, Life Senior Member, IEEE

MICHAEL REUTER, Member, IEEE

JAMES ZEIDLER, Fellow, IEEE
Spawar Systems Center San Diego

BRANDON ZEIDLER, Student Member, IEEE
University of California at San Diego

A low probability of intercept (LPI), or low probability of detection (LPD) communication technique known as cyclic code shift keying (CCSK) is described. We discuss the basic concepts of CCSK and describe a system based on the use of random or pseudorandom codes for biphase modulation. We use simulation to show that the bit error rate (BER) for CCSK can be closely estimated by using existing equations that apply to M-ary orthogonal signaling (MOS). Also, we show that significantly fewer computations are required for CCSK than for MOS when the number of bits per symbol is the same. We show that using biphase modulation results in waveforms that have a large time-bandwidth product and very low input signal-to-noise ratio (SNR) and thus inherently have an LPI by a radiometer. We evaluate detection by a radiometer and show that LPI can be achieved by using codes of lengths greater than about 2^{12} (i.e., by transmitting more than about 12 bits per symbol). Results illustrate the effect that the CCSK symbol length and error probability, and the radiometer integration time and probability of false alarm (PFA), have on detection by a radiometer. We describe a variation of CCSK called truncated CCSK (TCCSK). In this system, the code of length 2^k is cyclically shifted, then truncated and transmitted. Although shortened, the truncated code still represents k bits of information, thus leading to an increased data rate. We evaluate radiometer detection of TCCSK and it is shown that the probability of detection is increased compared with the detection of CCSK.

Manuscript received January 9, 2001; released for publication May 19, 2003.

IEEE Log No. T-AES/39/3/818481.

Refereeing of this contribution was handled by T. F. Roome.

This work was supported by the SSC San Diego In-House Independent Research Program and the SSC San Diego Independent Applied Research Program.

Authors' current addresses: G. M. Dillard, Spawar Systems Center San Diego, 53560 Hull St., San Diego, CA 92152-5001, E-mail: (george.dillard@navy.mil); M. Reuter, Motorola Automotive and Electronic Systems Group, Deer Park, IL; J. Zeidler and B. Zeidler, Dept. of Electrical and Computer Engineering, 9500 Gilman Dr., Mail Code 0407, University of California at San Diego, La Jolla, CA 92093-0407.

I. INTRODUCTION

Cyclic code shift keying (CCSK) is a form of M-ary signaling over a communication channel [1]. In its simplest form, a "base function" $f(t)$ is chosen, and a cyclically (circularly) shifted version of $f(t)$ is used to modulate a carrier. The function $f(t)$ has the property that its cyclic autocorrelation has a distinct peak and "low" sidelobes. Assuming synchronization, the receiver cyclically correlates the received signal plus noise with $f(t)$ and estimates the position of the correlation peak. If the number of resolvable positions is M, the number of bits per "symbol" is $B = \log_2 M$. The base function we consider here is a binary sequence $\mathbf{b} = (b_0, b_1, \ldots, b_{M-1})^T$ with $b_m = \pm 1$, resulting in biphase modulation of the carrier. We also describe a technique that increases the bit rate by using truncations of shifted versions of $\mathbf{b}$ to biphase modulate the carrier. This technique is referred to as truncated cyclic code shift keying (TCCSK).

Three methods for generating $\mathbf{b}$ are discussed, including a maximal-length sequence (MLS) [2], a modified maximal-length sequence (MMLS) [3] and a randomly chosen sequence. Maximal-length sequence generators produce sequences with elements +1 and 0, which we convert to ± 1 by replacing the zeros with -1. However, we use the term MLS to describe both types of sequences when the type is clear from the context.

Conventional M-ary orthogonal signaling (MOS) [4, p. 167 ff.] uses one of $M = 2^k$ orthogonal functions to modulate a carrier. The receiver correlates the received signal plus noise with each of the orthogonal functions and determines the one with the highest correlation. We show by Monte Carlo simulation that CCSK performance in Gaussian noise is essentially the same as MOS, when the symbol error probability P_S is larger than about 10^{-4}.

The primary reason for choosing CCSK for M-ary signaling instead of conventional MOS is the simplicity of the signal processing. We show that CCSK only requires the computation of the Fourier transform of the received signal plus noise followed by an inverse transform of the product of this transform and the complex conjugate of the transform of the base function. For the codes considered here, these operations are performed by using the discrete Fourier transform (DFT) or the fast Fourier transform (FFT). This is contrasted with the processing for MOS, which requires the correlation of each of the M orthogonal functions (e.g., Walsh functions) with the received signal plus noise.

The use of the binary sequence $\mathbf{b}$ described above as the base function leads to a system that provides a low probability of intercept (LPI) by a radiometer, because of the large processing gain. We briefly discuss the characteristics of a radiometer and derive the basic equations used to evaluate its performance.

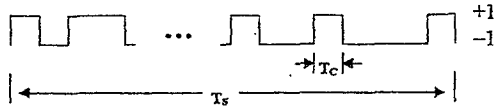


Fig. 1. Typical CCSK base function **b**.

These equations are then applied to the CCSK and TCCSK systems to evaluate their vulnerability to detection.

II. CYCLIC CODE SHIFT KEYING

CCSK uses discrete cyclic shifts of a base function $f(t)$ to modulate a carrier, with each shift representing B bits of information. The receiver determines the shift by computing the cyclic correlation of the base function $f(t)$ with the received signal plus noise. The base function we consider here is a binary sequence $\mathbf{b} = (b_0, b_1, \ldots, b_{M-1})^T$ with $b_m = \pm 1$, resulting in biphase modulation of the carrier. A typical sequence **b** is shown in Fig. 1. The elements of **b** indicated in Fig. 1 are called "chips." Each chip is of duration T_C and the "symbol" duration T_S is MT_C. We define the chip bandwidth as $W_C = 1/T_C$, so that $T_C W_C = 1$.

We consider three different methods for generating **b**. The first uses an MLS of length $M = 2^k - 1$, which has the property that its cyclic autocorrelation has a peak of M and sidelobes of -1. Unfortunately, in this case the number of bits B is less than k. Also, M is not a power of two, thus processing by using the FFT algorithm may be precluded. To alleviate these problems, an MMLS (also called an "extended m-sequence") [3] is used. In this case an MLS is generated and a -1 or $+1$ is inserted to extend the length to $M = 2^k$. A result of this modification is an increase in the level of the autocorrelation sidelobes, compared with the true MLS. We show later that this increase has little effect on error probabilities because the level of the input signals of interest is so low that the error process is controlled by the noise. This fact leads us to consider a third option in which **b** is obtained by generating a random binary sequence of ± 1 s.

A. Noncoherent CCSK Using Binary Sequences

The cyclic shifts of the code **b** are designated $\mathbf{b}_0, \mathbf{b}_1, \ldots, \mathbf{b}_{M-1}$, where $\mathbf{b}_0 = \mathbf{b}$, and $\mathbf{b}_n$ is the nth shift. We consider the case where it is reasonable to assume time synchronization so that the receiver knows the time of arrival of each "symbol" to a small fraction of one chip interval. We also assume that the carrier frequency is known. However, the relative phase of the received signal is not known, and noncoherent processing is required. We assume the received signal is a sum of signals of the form

$$r(t) = A\cos(\omega_0 t + \varphi_{mn} + \theta) + g(t) \qquad (1)$$

where A is the amplitude of the received signal, $\varphi_{mn} = 0$ or π is determined by the mth element of the transmitted code $\mathbf{b}_n$, θ is the unknown phase, and $g(t)$ is a Gaussian noise process with mean zero and (one-sided) power spectral density $N_0/2$. A quadrature (or baseband) detector is used and its sampled output is a column vector

$$\mathbf{r} = A\mathbf{b}_n \exp[j\theta] + \mathbf{g}. \qquad (2)$$

In (2), $\mathbf{b}_n$ is a column vector of the shifted code elements, **g** is a column vector of independent and identically (IID) circular Gaussian noise with variance σ^2, and A is the signal amplitude. The receiver computes

$$S_m = |\mathbf{b}_m^T \mathbf{r}| = |A\mathbf{b}_m^T \mathbf{b}_n + \mathbf{b}_m^T \mathbf{g}| \qquad (3)$$

for $m = 0, 1, \ldots, M-1$. If $\max\{S_m\} = S_p$, the bits corresponding to the pth symbol are output. A symbol error occurs if $p \neq n$.

B. Comparisons with M-ary Orthogonal Signaling

In conventional MOS, one of a set of M orthogonal, equal-energy signals is used to represent $B = \log_2 M$ bits of information. One form of the receiver correlates the received signal plus noise with each of the M reference signals and determines which has the maximum correlation. Although a single cyclic correlation is performed in implementing CCSK, the process can be viewed as the performance of M separate correlations, as implied in (3). If the cyclic shifts of the code were all uncorrelated, then CCSK would be a special case of MOS. However, for codes that provide LPI, the cyclic shifts are correlated; that is, the cyclic autocorrelation function has non-zero "sidelobes." We show that the bit error rate (BER) for CCSK can be approximated by using the equations for MOS, even though the cyclic shifts are correlated.

C. Performance Estimates

The performance of noncoherent MOS in terms of BER is well documented in the literature [5, p. 489]. For M orthogonal signals, the probability of a symbol (or word) error is given by

$$P_S = 1 - \int_0^\infty \exp[-(x+q)] I_0(\sqrt{4qx}) H(x) dx \qquad (4a)$$

where

$$H(x) = [1 - e^{-x}]^{M-1} \qquad (4b)$$

$q = E_S/N_0$ is the ratio of symbol energy to noise power spectral density, and $I_0(x)$ is the modified Bessel function of the first kind and order zero. By using the binomial expansion of $H(x)$ and integrating (4a) term-by-term, a finite series for P_S is obtained [5, p. 489]. However, the series is alternating in sign

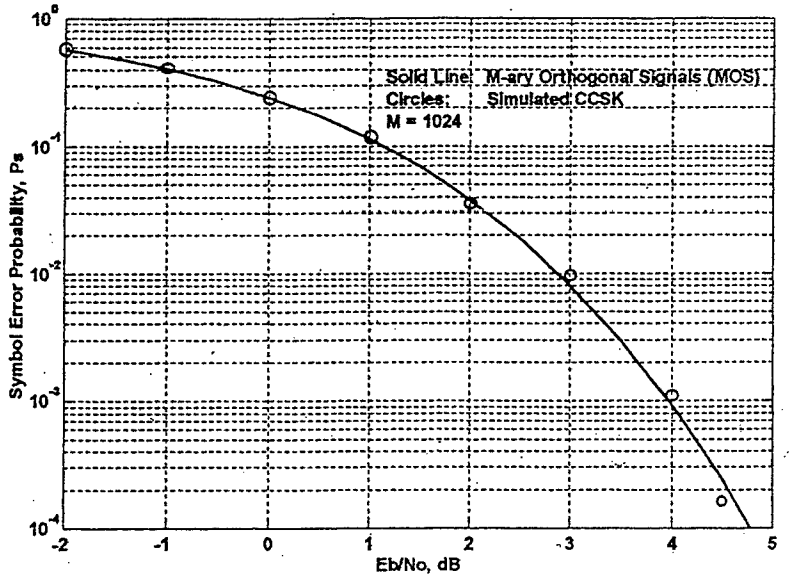


Fig. 2. Comparison of CCSK performance with MOS, $M = 1024$.

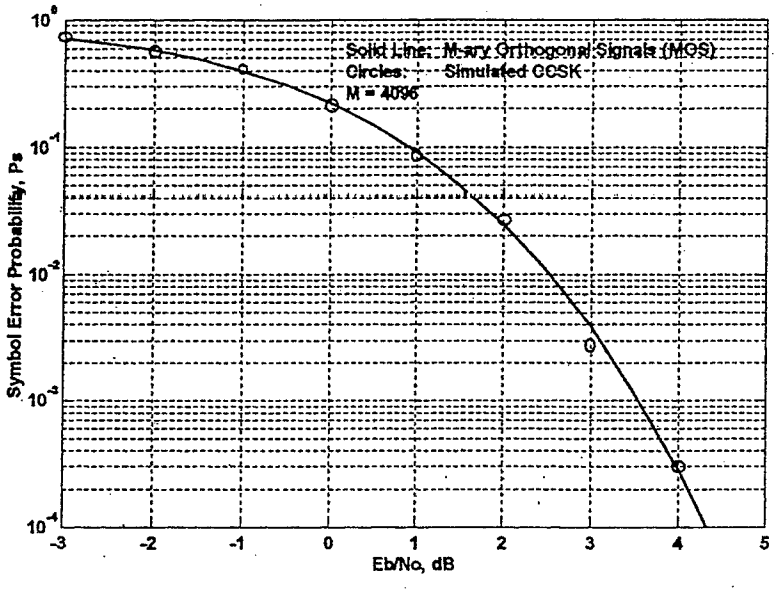


Fig. 3. Comparison of CCSK performance with MOS, $M = 4096$.

and presents numerical difficulties for large M or q. Fortunately, (4a) lends itself to numerical integration, and that is the technique we use for its evaluation. With $M = 2^k$, the probability P_B of a bit error is obtained directly from P_S as [5, p. 198]

$$P_B = P_S \frac{2^{k-1}}{2^k - 1}. \tag{5}$$

Monte Carlo simulations were performed to compare CCSK performance with MOS. Some of the results are shown in Figs. 2–4. From these results we conclude that (4) can be used as a close approximation to the symbol error probability for CCSK when P_S is larger than about 10^{-4} and when $M \geq 1024$. This conclusion is based on the simulations performed; however, there appears to be no reason to assume that the approximation is not valid for smaller P_S, especially for large values of M. To corroborate the simulation results, we show that the cross-correlation between cyclic shifts are small and thus are "approximately" orthogonal. Table I shows the maximum cross-correlation for $k = 9, 10, \ldots, 16$ for MLS, MMLS, and random sequences. The MMLS results were obtained by using a single set of shift-register taps for each k to generate the sequence. Some slight variations are expected if other sets of taps are used. Note that for $k \geq 12$, the maximum cross-correlation is less than 0.03 for MMLS and decreases with increasing k. The tabulated value for each random sequence was obtained by averaging the results from 100 different random sequences. A comparison shows that the random sequence has larger maximum cross-correlation than

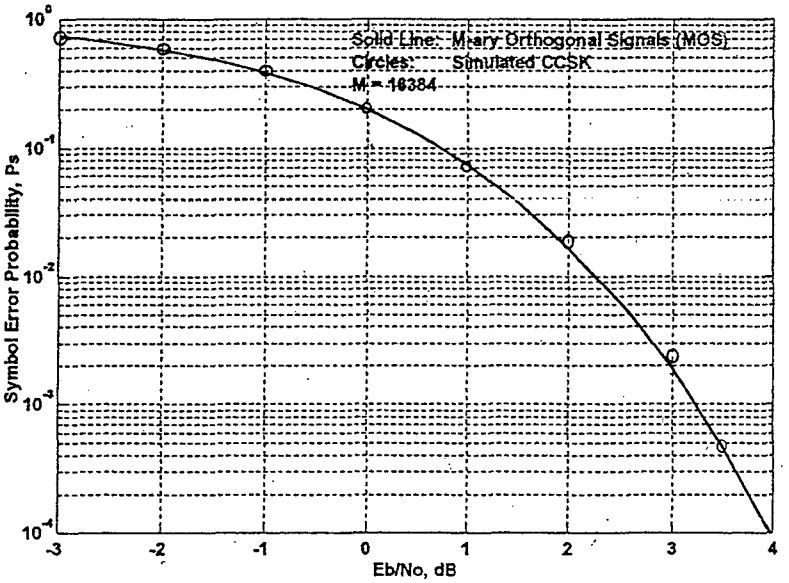


Fig. 4. Comparison of CCSK performance with MOS, $M = 16384$.

TABLE I
Maximum Cross-Correlation of Cyclic Shifts, $M = 2^k$

k	9	10	11	12	13	14	15	16
MLS	0.002	0.001	0.0005	0.0002	0.0001	$2^{-14}-1$	$2^{-15}-1$	$2^{-16}-1$
MMLS	0.0625	0.0586	0.0391	0.0254	0.0225	0.0173	0.0104	0.0082
RANDOM	0.1361	0.1012	0.0760	0.0563	0.0422	0.0308	0.0228	0.0167

the MMLS. As expected, the MLS has the least cross-correlation.

The simulation results presented in Figs. 2–4, along with the data in Table 1, give credence to concluding that the error probabilities for MOS are good estimates of those for CCSK. This is especially true for larger values of k because, as indicated, the maximum cross-correlation decreases for both MMLS and random sequences. Also, this estimate is applicable when the input signal-to-noise ratio (SNR) is low and the additive noise obscures the non-zero cross-correlation between the cyclic shifts of **b**.

D. Implementation Issues

Equation (3) is a representation of the processing required by the receiver and is useful in comparisons with MOS. However, in practice we compute the cyclic correlation by using the DFT. The DFT of the code **b** is computed and its complex conjugate is stored. The receiver computes the DFT of the sampled received signal **r**, which is defined in (2), and obtains

$$\mathbf{S} = |\mathrm{IDFT}(\mathrm{DFT}^*(\mathbf{b}) \times \mathrm{DFT}(\mathbf{r}))| \qquad (6)$$

where IDFT is the inverse DFT. (The multiplication implied in (6) is term-by-term.) The elements of the vector **S** obtained by using (6) are $S_0, S_1, \ldots, S_{M-1}$, which are the same as are obtained by using (3). From (6), it follows that the processing required for CCSK can be significantly less than for MOS, which requires the computation of all M individual cross-correlations.

E. TCCSK

The CCSK system previously described transmits all M elements (chips) of cyclic shifts of the code **b** to represent symbols. Thus, the data rate is $1/T_S$ symbols per second, or k/T_S bits per second. (See Fig. 1.) We may increase the bit rate while maintaining the same bandwidth by using the technique we refer to as TCCSK. As discussed in the next section, the code sequence **b** is chosen to have the property that its cyclic autocorrelation has a distinct peak and low sidelobes. If the code length is large (e.g., $M \geq 1024$), then a subsequence $\mathbf{b}_T$ of **b** exhibits these properties when cyclically correlated with **b**. This fact leads to the use of TCCSK.

Instead of transmitting all M chips of the shifted code $\mathbf{b}_n$ to represent the nth symbol, the code $\mathbf{b}_n$ is truncated and only the first M_T chips $\mathbf{b}_{nT}$ of $\mathbf{b}_n$ are transmitted. The received signal plus noise is cyclically correlated with **b** by first appending $M - M_T$ zeroes to $\mathbf{r}_T = A\mathbf{b}_{nT}\exp[j\theta] + \mathbf{g}_T$. (See (2).) As a result, the number of bits per symbol is still k but the bit rate has been increased by a factor of M/M_T. If TCCSK is to maintain the same BER as CCSK, then E_S/N_0 must be the same for both. This means that the

amplitude of the signal must be increased by a factor of $(M/M_T)^{1/2}$. This is considered later when detection by a radiometer is discussed.

III. CODE SELECTION TRADEOFFS

For CCSK, the information transmitted is contained in the location of the maximum of the correlation function defined by (3) and (6). Thus, a measure of performance that can be used in code selection is the peak-power to mean-sidelobe-power ratio (PMR). If code $\mathbf{b}'$ has a significantly higher PMR than code $\mathbf{b}''$, then it is intuitive that $\mathbf{b}'$ will provide better performance. Another consideration in code selection is their noise-like property. MLSs are sometimes referred to as "pseudonoise" sequences, but they possess certain structure not found in a truly random sequence. In an MLS (with elements 1 and 0) of length $M = 2^k - 1$, all k-bit binary numbers except zero appear as k successive elements. For example, one MLS of length seven is $\mathbf{b} =$ [1 0 1 0 0 1 1]. Each three successive bits are binary representations of [5 2 4 1 3 7 6], with the last two [7 6] determined cyclically. Some of this same structure still is retained if an MMLS is used.

A. PMR

To simplify the analysis in defining and evaluating the PMR of a sequence $\mathbf{b}$, we assume that the phase of the received signal is known. In this case, the received signal plus noise is $\mathbf{r} = A\mathbf{b}_n + \mathbf{g}$, where $\mathbf{g}$ is a vector of IID Gaussian noise with variance σ^2. Without loss of generality, we may assume that $n = 0$; i.e., assume that $\mathbf{b}_n = \mathbf{b}$. The correlation of $\mathbf{r}$ with $\mathbf{b}$ produces M terms. The first term, defined as the "peak," is

$$s_0 = MA + h_0 \tag{7}$$

where h_0 is a Gaussian random variable with mean zero and variance $M\sigma^2$. The remaining $M - 1$ terms (the sidelobes) are of the form

$$s_m = q_m A + h_m \tag{8}$$

where q_m is the mth signal sidelobe and h_m is a Gaussian random variable with mean zero and variance $M\sigma^2$. We define PMR as

$$\text{PMR} = \frac{E[s_0^2]}{AV\{E[s_m^2]\}} \tag{9}$$

where AV denotes the average over the $M - 1$ sidelobes. Note that we define the peak to be located at the position of the shifted code (in this case, zero); however, for low SNR, the actual maximum may occur at some other position (i.e., an error occurs). By using (7), (8), and (9), the PMR is given by

$$\text{PMR} = \frac{M^2A^2 + M\sigma^2}{QA^2 + M\sigma^2} \tag{10}$$

where Q is the average sidelobe power of the code $\mathbf{b}$. Equation (10) can be written as

$$\text{PMR} = \frac{1 + M\text{SNR}_{\text{IN}}}{1 + Q\text{SNR}_{\text{IN}}/M} \tag{11}$$

where $\text{SNR}_{\text{IN}} = A^2/\sigma^2$ is the input SNR.

Fig. 5 shows PMR versus SNR_{IN} for an MLS, MMLS, and a random binary (RANDOM) sequence. Note that the MLS curve is basically a unity-slope line up to about 20 dB input SNR. What is most striking, however, is the fact that the three curves are nearly coincident for negative input SNR, which is the usual case for use in CCSK. Also, it is obvious from the figure that a unity-slope line provides an excellent estimate of PMR for the region of interest (negative input SNR). Further results in the next figure illustrate these points.

The PMR versus SNR_{IN} for $M = 2^{10}$, 2^{13} and 2^{16} is shown in Fig. 6 for a random sequence and an MMLS. Note that the three pairs of curves follow the unity-slope line up to SNR_{IN} of about -5 dB. An exception is the curve for 2^{10} when SNR_{IN} is less than about -20 dB, the region where the position of the peak correlation is likely to be determined by noise. That is, the peak does not necessarily occur at $n = 0$.

B. PMR for TCCSK

When TCCSK is used it is necessary to modify (11) to compute the PMR. Because only M_T chips of the code are transmitted, the peak correlation is given by

$$s_{0T} = M_T A + h_{0T} \tag{12}$$

where h_{0T} is a Gaussian random variable with mean zero and variance $M_T\sigma^2$. Similarly, the sidelobes are of the form

$$s_{mT} = q_{mT} A + h_{mT} \tag{13}$$

where q_{mT} is the mth signal sidelobe and h_{mT} is Gaussian with mean zero and variance $M_T\sigma^2$. Therefore, the PMR of the truncated sequence is

$$\text{PMR}_T = \frac{1 + M_T\text{SNR}_{\text{IN}}}{1 + Q_T\text{SNR}_{\text{IN}}/M_T} \tag{14}$$

where Q_T is the average sidelobe power of the truncated code.

Fig. 7 shows PMR_T as a function of the input SNR for $M = 2^{13}$ and $M_T = 2^{13}$, 2^{12}, and 2^{11}. (When $M_T = 2^{13}$, there is no truncation.) This shows that PMR_T decreases by about 3 dB when M_T is decreased by a factor of two. However, this fact is misleading

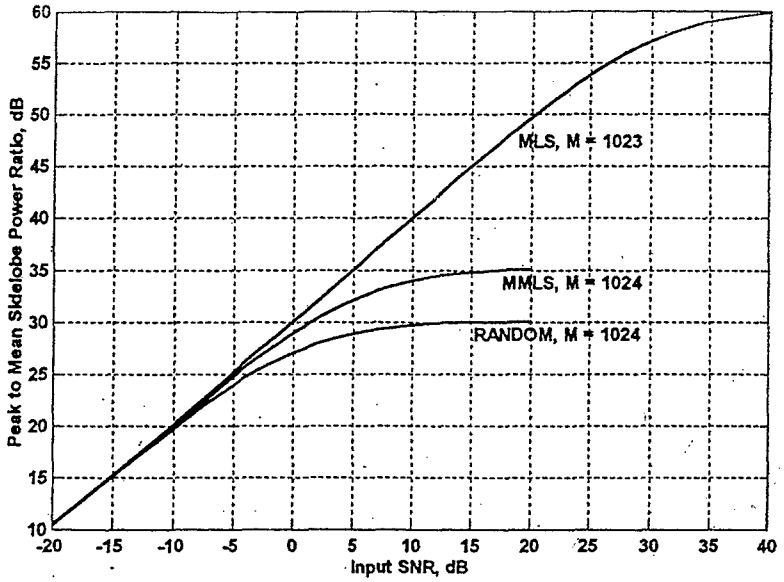


Fig. 5. PMR versus input SNR for CCSK.

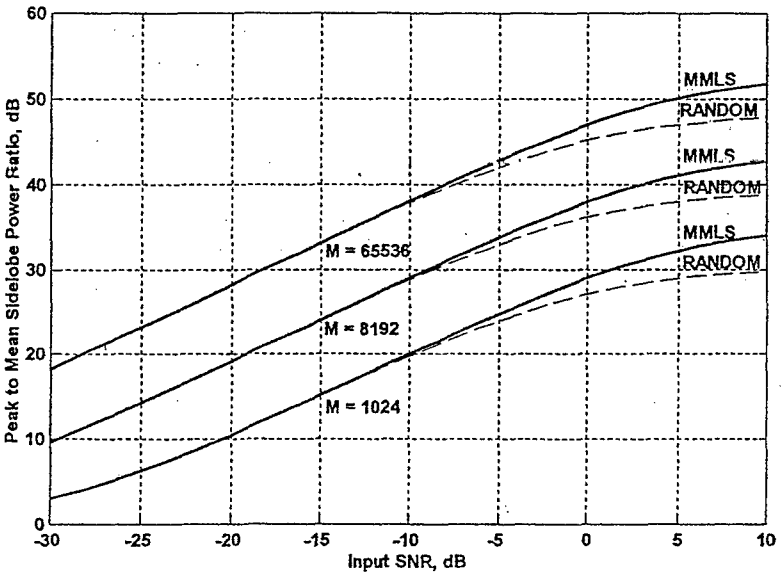


Fig. 6. PMR versus input SNR for CCSK.

when error performance is considered. To maintain the same error performance, E_B/N_0 must be kept constant when M_T is decreased; that is, the input SNR must increase. Fig. 8 shows PMR_T as a function of E_B/N_0 over the range of 0 to 20 dB. Note that for small E_B/N_0, PMR_T is essentially the same for both truncated and nontruncated sequences. In fact, as shown in the next section, the range of interest for E_B/N_0 is about 0 to 5 dB, and over this range PMR and PMR_T differ by only a fraction of a dB.

C. Random versus Pseudorandom Codes

By observing graphs of the probability of a bit error P_B versus E_B/N_0 (e.g., [5, Fig. 10-6]) we see that for $10 \le k \le 20$ and $0.00001 \le P_B \le 0.1$, the required E_B/N_0 is less than about 4.5 dB. Also, E_B/N_0 (in dB) is given by

$$E_B/N_0 = \text{SNR}_{\text{IN}} + 10\log_{10}M - 10\log_{10}k \quad (15)$$

which means that SNR_{IN} is less than about -15.6 dB. (For TCCSK, E_B/N_0 is given by (15) with M replaced by M_T.) The data in Fig. 6 show that the PMR for MMLS and a random sequence is essentially the same over the range of SNR_{IN} of interest. Therefore, random sequences can be used as the code in CCSK with little effect on performance compared with MMLS.

Some caution must be used in generating a random sequence for the CCSK code. For example, although

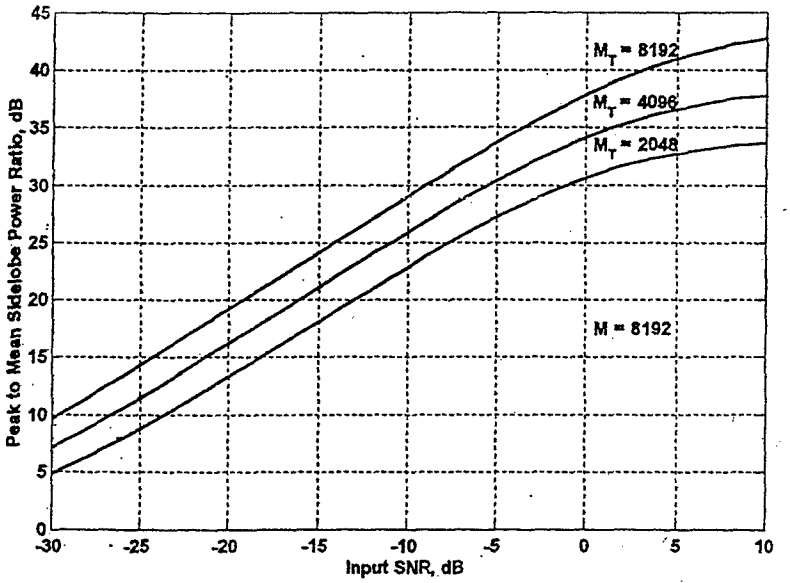


Fig. 7. PMR_T versus input SNR for TCCSK.

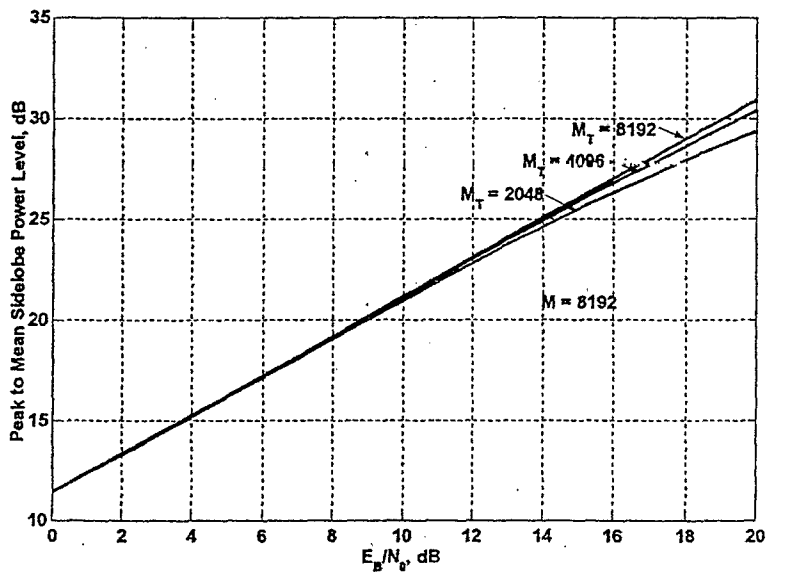


Fig. 8. PMR_T versus E_B/N_0 for TCCSK.

the sequence is called "random," it is likely to be obtained by using a random number generator that is actually "pseudorandom." Thus the quality of the generator used must be ensured [6]. (The random codes used in Figs. 5 and 6 were generated by using the Matlab^R routine "rand.") Additionally, some random codes may have unacceptable properties. For example, it may be necessary to ensure that the numbers of 1 s and -1 s are approximately equal to avoid having a dc offset.

IV. VULNERABILITY OF CCSK TO RADIOMETER DETECTION

A radiometer (or energy detector) is often the most effective device to detect spread-spectrum signals [7]. It is conceptually a simple device, and requires only a few assumptions to be made about the structure of the signals being detected. Invulnerability to detection by a radiometer is required if a communication system is to be considered LPI. Fig. 9 is a simplified block diagram of a radiometer.

A. Equations for Evaluating Performance

Equations for evaluating radiometer performance are given in [7] and are based on derivations by Urkowitz [8]. We assume that the noise at the input to the radiometer is a zero-mean, stationary, Gaussian random process that has a flat, bandlimited (one-sided) power spectral density $N_0/2$ over the bandwidth W of the bandpass filter. For convenience,

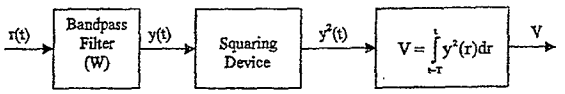


Fig. 9. Radiometer block diagram.

we consider a normalized detection statistic $V' = 2V/N_0$. Urkowitz shows that the probability distribution of V' is closely approximated by the chi-square distribution with $2TW$ deg of freedom in the noise-only case and by the noncentral chi-square distribution with $2TW$ deg of freedom and noncentrality parameter $\lambda = 2E_R/N_0 = 2S$ in the signal-plus-noise case. The parameter E_R is the total signal energy integrated by the radiometer and N_0 is the noise power spectral density. For simplicity, we assume that TW is an integer.

Detection is accomplished by comparing the normalized radiometer output V' with a threshold K, and a signal is claimed present if $V' \geq K$. If $V' \geq K$ when no signal is present, a false alarm occurs. By making appropriate changes of variables in the central and noncentral chi-square distributions, and defining $K_0 = K/2$, the equations for the probability of a false alarm PFA and the probability of detection P_D are given by [7, pp. 56–57]

$$\text{PFA} = \int_{K_0}^{\infty} \frac{u^{TW-1}e^{-u}}{(TW-1)!}du \tag{16}$$

and

$$P_D = \int_{K_0}^{\infty} \left(\frac{u}{S}\right)^{(TW-1)/2} e^{-(u+S)} I_{TW-1}(2\sqrt{uS})du \tag{17}$$

where $I_{TW-1}(x)$ is the modified Bessel function of the first kind and order $TW-1$. These equations were used to evaluate the detectability of the CCSK biphase modulated waveforms considered here.

B. Radiometer Detection of CCSK

To simplify the analysis, we assume that the radiometer has the same gains and losses as the intended communications receiver, and is located at the same range. As a result of this assumption both have the same SNR_{IN}, so that $E_R = E_S$ when $T = T_S$. We also assume that the radiometer integration time varies in units of the chip time T_C. Then, because $T_C W_C = 1$, the radiometer TW product is just the number of chips integrated. Also, E_R/N_0 (in dB) can be expressed as

$$E_R/N_0 = \text{SNR}_{\text{IN}} + 10\log_{10} TW. \tag{18}$$

By using (15) and (18), we have the following relation between E_R/N_0 and E_B/N_0:

$$E_R/N_0 = E_B/N_0 + 10\log_{10} TW - 10\log_{10} M + 10\log_{10} k. \tag{19}$$

Because $E_S/N_0 = E_B/N_0 + 10\log_{10} k$,

$$E_R/N_0 = E_S/N_0 + 10\log_{10} TW - 10\log_{10} M. \tag{20}$$

If q symbols are transmitted contiguously, then (18)–(20) apply when $TW \leq qM$. If $TW > qM$, then the radiometer parameters are TW and $E_R/N_0 = E_S/N_0 + 10\log_{10} q$.

When the symbol error probability P_S and the number of bits k are specified, the required E_S/N_0 for CCSK is determined by solving (4). Equation (20) is then solved for $S = E_R/N_0$ and (16) and (17) are used to determine the detection probability P_D achieved by the radiometer for a given PFA. Results presented later take into account the effect of holding the false-alarm rate (FAR) a constant.

We first assume that the radiometer integrates over T_S seconds, the length of one CCSK symbol, with the integration interval matched to the symbol. This results in $E_S = E_R$ and radiometer time-bandwidth product $TW = M$. Table II shows the detection probability P_D for the indicated number of bits k, when $P_S = 0.001$ and PFA = 0.0001.

The data in Fig. 10 exhibit further the vulnerability of CCSK to detection by a radiometer when $TW = M$. Three sets of curves are shown for three choices of PFA. Within each set, the symbol error probability P_S varies from 0.00001 to 0.1. From these sets of curves it is obvious that vulnerability to detection decreases with M, but increases with increasing radiometer PFA or with decreasing symbol error probability P_S. Also included is the spectral efficiency R/W (in bits per second per hertz of bandwidth) [8, pp. 282–284], which is a measure of performance of modulation methods. For this case, the spectral efficiency is given by

$$R/W = \frac{\log_2 M}{M}. \tag{21}$$

Note that the vulnerability to detection increases with increasing spectral efficiency. Also, the values of PFA used in Fig. 10 are likely to be larger than would be used in practice. However, the trend is obvious: a further decrease in PFA will lead to a decrease in P_D when other parameters remain the same as used in the figure.

We now assume that symbols are transmitted continuously (and are contiguous). An assumption more realistic than the one above ($TW = M$) is that the radiometer integrates over multiple symbols. In this case, its probability of detection increases compared with the single symbol case. Conversely, if the radiometer integration time is less than the length of one symbol, the probability of detection is decreased. This is illustrated by the data in Fig. 11, which shows the probability of detection by a radiometer as its time-bandwidth product (i.e., integration time) varies. For each k (k = 10, 12, 14, and 16) results are shown for a range of values of P_S, and the circles represent the results given in Table II. Note that P_D increases

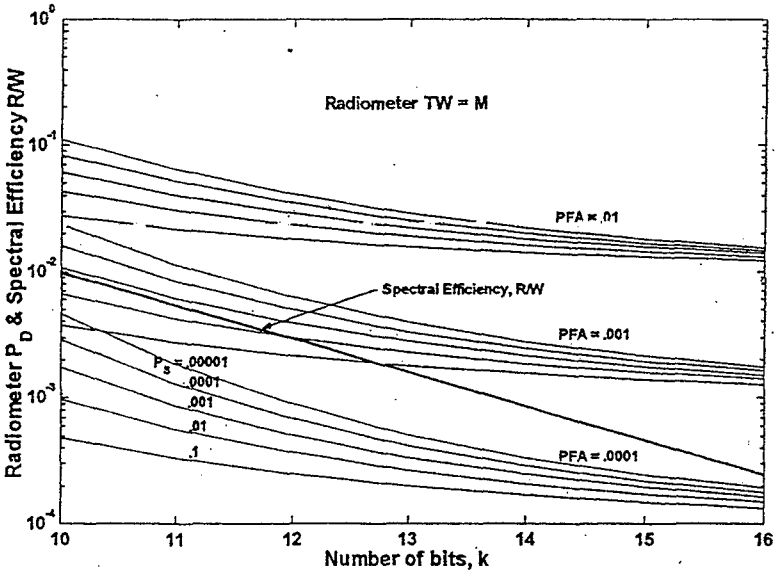


Fig. 10. Spectral efficiency and radiometer detection of CCSK.

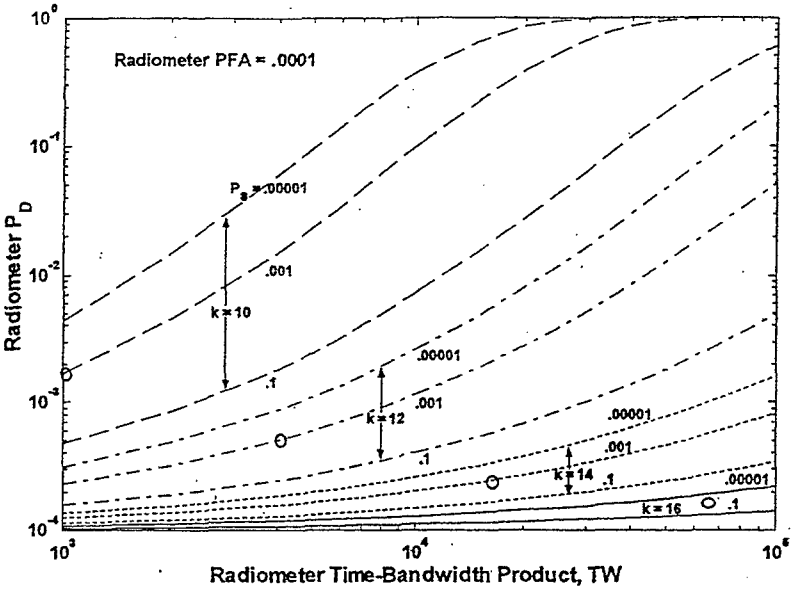


Fig. 11. P_D versus TW for radiometer detection of CCSK.

TABLE II
Probability of Detection by Radiometer with Integration Time T_S

Number of bits, k	Required E_B/N_0 (dB)	E_S/N_0 (dB)	P_D
10	3.97	13.97	0.00170
12	3.56	14.35	0.00051
14	3.24	14.70	0.00024
16	2.97	15.01	0.00016

considerably with increasing TW and decreasing P_S for $k = 10$ and $k = 12$. However, for $k = 14$ and $k = 16$, the variation of P_D with TW and P_S is small. Thus, to simultaneously achieve LPI performance (low P_D) for small values of P_S requires the use of long sequences with lowered spectral efficiency R/W.

C. Radiometer Detection of TCCSK

When TCCSK is used, the equation for E_R/N_0 is given by (19) with M replaced by M_T:

$$E_R/N_0 = E_B/N_0 + 10\log_{10} TW - 10\log_{10} M_T + 10\log_{10} k. \tag{22}$$

We first assume that the radiometer integrates over the truncated symbol length; i.e., $TW = M_T$. Results are only given for $k = 16$ ($M = 65536$), and illustrate the effect of truncation on vulnerability to detection by a radiometer.

Fig. 12 shows P_D versus the truncated symbol length M_T for the case where $TW = M_T$. Three sets of curves are shown for three values of PFA. Within each set the symbol error probability varies from 0.00001 to 0.1. Also shown is the spectral efficiency. The

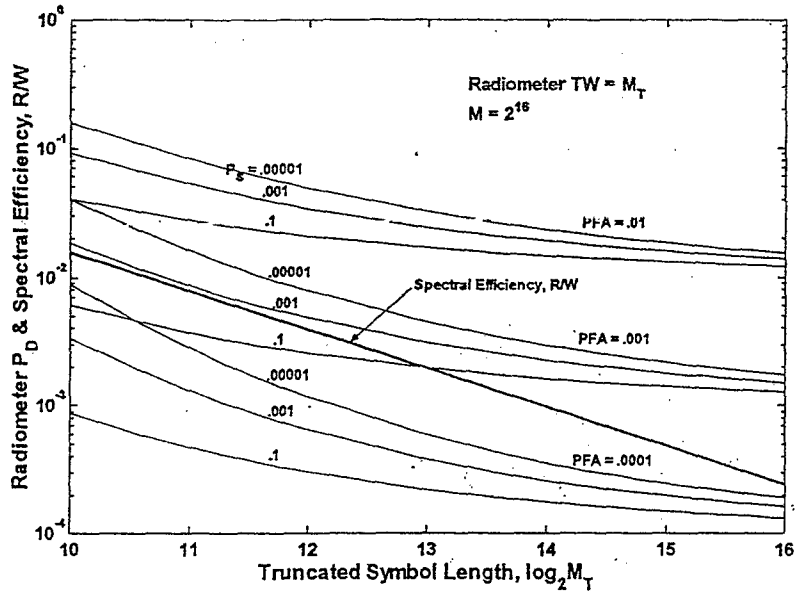


Fig. 12. P_D and spectral efficiency versus truncated symbol length M_T.

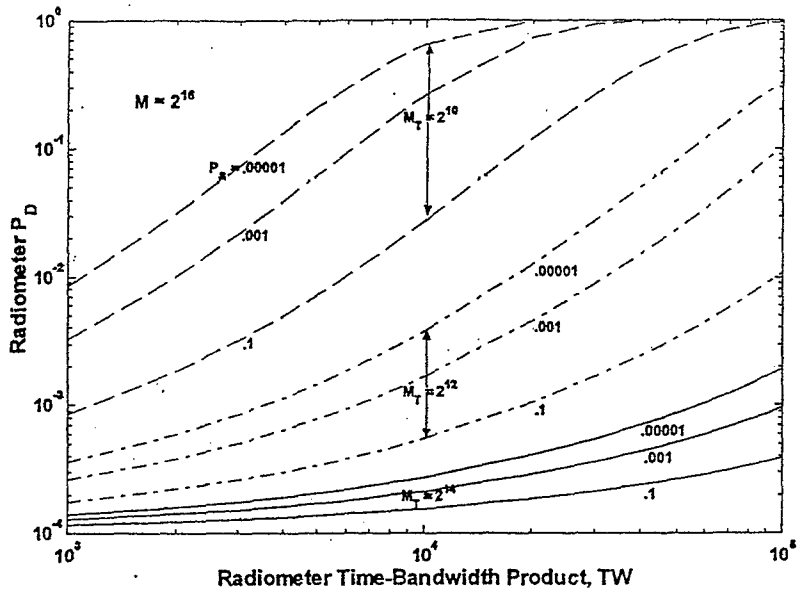


Fig. 13. P_D versus TW for radiometer detection of TCCSK.

results in Fig. 9 and Fig. 11 show that the detectability of TCCSK increases slightly compared with CCSK when the transmitted symbol lengths are the same. Also, TCCSK slightly increases the spectral efficiency for small symbol lengths. This occurs because the number of bits per symbol is a constant for TCCSK (16 in the case shown), but varies for CCSK. Again, the values of PFA used are likely to be larger than in practice, but the trend is obvious.

Fig. 13 shows P_D versus TW for $M = 2^{16}$ and for $M_T = 2^{10}$, 2^{12}, and 2^{14} and PFA = 0.0001. For each choice of M_T, curves are shown for a range of values of P_S. We again assume that symbols are transmitted continuously (and are contiguous). A comparison of Fig. 13 with Fig. 11 shows that, for the same symbol length (i.e., $M_T = 2^k$), the detectability of TCCSK increases considerably compared with CCSK for $M_T = 2^{10}$, but only slightly for longer sequences.

D. FAR

For the detection results presented above, the radiometer PFA is held constant. It is usually more realistic to hold the FAR constant, especially when comparing systems with different integration times. We define the FAR as the average number of false alarms per second (or some other unit of time). Its effect on detectability is discussed in detail in [7] and is summarized here.

We assume that the integrator shown in Fig. 9 operates in the integrate-and-dump mode. That is,

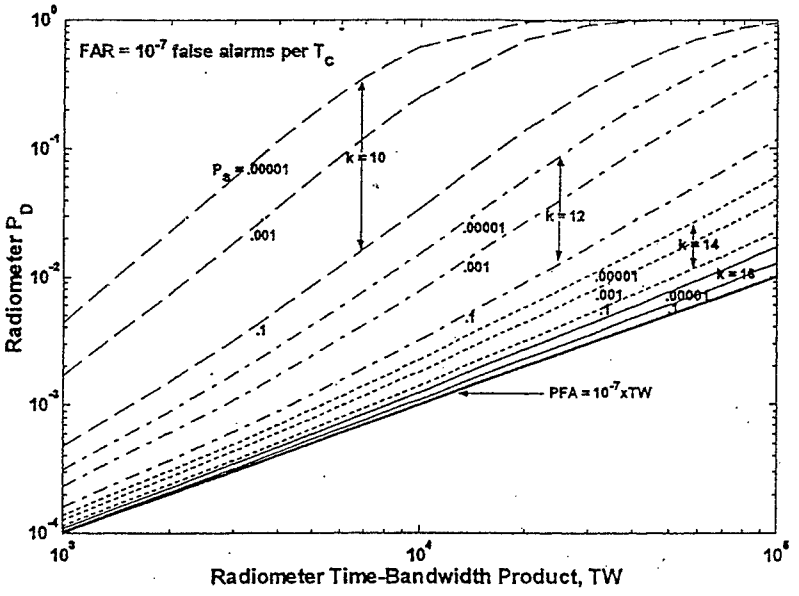


Fig. 14. P_D versus TW for CFAR radiometer detection of CCSK.

the integrator output is sampled every T seconds, the integrator is reset to zero, then integrates over the next T seconds, etc. Thus, a decision is made every T seconds and the false-alarm rate is FAR = PFA/T. If a fixed FAR is required and we compare two systems with integration times T_1 and T_2 ($T_1 \neq T_2$), we must use a different PFA for each system. This is true even if the bandwidths of the two systems are equal. Conversely, if the integration times of the two systems are equal, the FAR is independent of their bandwidths. However, detection performance does depend on their bandwidths because (16) and (17) depend on the TW product.

Fig. 14 illustrates the effect a constant FAR (CFAR) has on radiometer detection of CCSK and should be compared with Fig. 11, in which a constant PFA (CPFA) is assumed. In Fig. 14, FAR = 10^{-7} and is expressed in units of T_C; thus, PFA increases linearly with FAR. The results for both cases (CFAR and CPFA) are identical for $TW = 1024$; however, for $TW > 1024$, P_D is larger for CFAR and for $TW < 1024$, P_D is larger for CPFA. These situations occur because P_D increases with increasing PFA (and vice versa) when TW and E_R/N_0 are constant. Also, because P_D is bounded below by PFA and PFA increases with increasing TW, P_D approaches 1.0 asymptotically as TW increases. This effect is evident in the results shown in Fig. 14.

Although not shown, similar results are obtained for detection of TCCSK by a CFAR radiometer. That is, if the results in Fig. 13 for CPFA were compared with the corresponding results for CFAR, the same conclusions made just above would apply.

V. CONCLUSIONS

A low probability of intercept (LPI) communication technique known as CCSK has been described and discussed. This technique uses cyclic (circular) shifts of a base function $f(t)$ to modulate a carrier. The function $f(t)$ has the property that its cyclic autocorrelation has a distinct peak and low sidelobes. The receiver estimates the position of the peak correlation of the received signal plus noise with $f(t)$. If there are M resolvable positions the estimated position represents $B = \log_2 M$ bits.

The base functions considered are binary sequences of +1 s and −1 s, which results in biphase modulation of the carrier. Three different methods for generating these sequences were evaluated in terms of their PMR. The first is an MLS of length $M = 2^k - 1$, which has the property that its cyclic autocorrelation has a peak of $M - 1$ and sidelobes of magnitude 1. Because the MLS only represents $k - 1$ bits, an MMLS was considered. The MMLS is obtained by appending a +1 or −1 to a MLS, thus resulting in a sequence of length 2^k that represents k bits. Both the MLS and MMLS have well-defined structure and this led to the consideration of a random sequence of length 2^k. Results showed no significant difference in communication performance when comparing the use of an MMLS with a random sequence.

Simulation results were obtained to show that that the performance of CCSK in terms of probability of symbol error P_S and required E_B/N_0 can be measured by using equations that apply to MOS. Also, it was shown that the receiver signal processing for CCSK is simpler and easier to implement than for MOS because only one cyclic correlation is computed for CCSK.

A generic radiometer system was defined and equations for evaluating its detection performance were given. These equations were applied to evaluate the detection of CCSK and TCCSK. Results given for various combinations of parameters show that

to achieve LPI performance, transmitted symbols of length greater than about 2^{12} are required. The use of TCCSK results in a data rate higher than CCSK, but with a penalty of higher detectability. The tradeoffs between detectability and data rate for a particular application must be made on a case-by-case basis. However, we conclude that CCSK and TCCSK provide LPI capabilities and are techniques that are simple and easy to implement.

REFERENCES

[1] Endsley, J. D., and Dean, R. A. (1994)
Multi-access properties of transform domain spread spectrum systems.
In *Proceedings of the 1994 Tactical Communications Conference, Vol. 1, Digital Technology for the Tactical Communicator*, 1994, 505–506.

[2] Dixon, R. C. (1994)
Spread Spectrum Systems with Commercial Applications (3rd ed.).
New York: Wiley, 1994.

[3] Fiebig, U. C. G., and Schnell, M. (1993)
Correlation properties of extended M-sequences.
Electronic Letters, **29**, 20 (Sept. 1993), 1753–1755.

[4] Sklar, B. (1988)
Digital Communications Fundamentals and Applications.
Englewood Cliffs, NJ: Prentice-Hall, 1988.

[5] Lindsey, W. C., and Simon, M. K. (1973)
Telecommunication Systems Engineering.
Englewood Cliffs, NJ: Prentice-Hall, 1973.

[6] Park, S. K., and Miller, K. W. (1988)
Random number generators: Good ones are hard to find.
Communication of the A. C. M., **32**, 10 (Oct. 1988), 1192–1201.

[7] Dillard, R. A., and Dillard, G. M. (1989)
Detectability of Spread Spectrum Signals.
Norwood, MA: Artech House, 1989.

[8] Urkowitz, H. (1967)
Energy detection of unknown deterministic signals.
Proceedings of the IEEE, **55**, 4 (Apr. 1967), 523–531.

[9] Proakis, J. G. (1995)
Digital Communications (3rd ed.).
New York: McGraw-Hill, 1995.

George M. Dillard (M'67—SM'69—LSM'00) was born in Little River, TX on November 12, 1931. He received the A.B. and M.S. degrees in mathematics from San Diego State College, San Diego, CA in 1959 and 1962 and the Ph.D. in information and computer science from the University of California at San Diego in 1971.

Since April 1959, he has worked as a mathematician at the Space and Naval Warfare Systems Center, San Diego (SSCSD) and it predecessor organizations. His primary research activities involved the application of distribution-free and nonparametric statistics, sequential analysis, detection theory, and other statistical techniques to signal detection for radar and communication systems. He also participated in programs that included radar signal processing, ECCM techniques for radar, inverse synthetic aperture radar, and the technical evaluation of surveillance systems developed for the Navy. His recent research has been in evaluating the detectability of spread-spectrum signals and he is the coauthor of one book and author or coauthor of several papers in that area. He retired from the Federal Service in January 1991, but has continued part time work as a reemployed annuitant in the SSCSD Joint and national Systems Division.

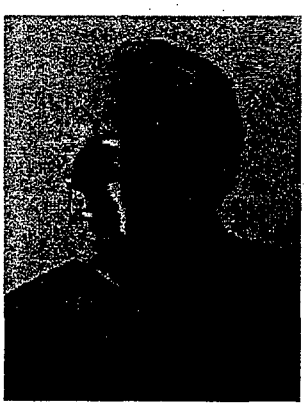
Michael Reuter (S'82—M'86) received the B.S. and M.S. degrees in electrical engineering from the University of Illinois, Urbana-Champaign, in 1984 and 1986, respectively, and the Ph.D. degree in electrical and computer engineering from the University of California, San Diego, in 2000.

From 1987 to 2002 he was with the Space and Naval Warfare Systems Center, San Diego, CA, where his research interests were in adaptive and statistical processing applied to problems in wireless communications. Since 2002, he has been with the Motorola Automotive and Electronics Systems Group, Deer Park, IL.

Brandon Zeidler is currently a Ph.D. student at the University of California, San Diego. He earned his M.S. degree in electrical and computer engineering with an emphasis in communications theory and systems from University of California, San Diego, (UCSD) in 2002. He attended the University of California, Santa Barbara (UCSB) with a four year, full-tuition Regents scholarship and completed his B.S. degree in electrical and computer engineering in 1999.

He has worked two consecutive summers at four high-tech companies in San Diego: Alliant Techsystems, Digital Transport Systems, TRW Avionics Systems Division, and SPAWAR Systems Center.

Mr. Zeidler's involvement in undergraduate research was recognized with a President's Undergraduate Research Fellowship and a scholarship from the National Society of Professional Engineers. He graduated Cum Laude and was selected as the student speaker for the UCSB College of Engineering commencement ceremony. At UCSB he served as president of the Engineering Student Council and the Eta Kappa Nu honor society, and as an officer for Tau Beta Pi. He currently serves as an officer of the Graduate Student Council at UCSD.



James R. Zeidler (M'76—SM'84—F'94) has been a scientist at the Space and Naval Warfare Systems Center, San Diego, CA since 1974. Since 1988, he has also been an adjunct professor of electrical and computer engineering at the University of California, San Diego. His research interests include communications signal processing, adaptive signal processing and array processing applied to wireless communications systems.

Dr. Zeidler was an associate editor of the *IEEE Transactions on Signal Processing* from 1991 to 1994. He received the Lauritsen-Bennett award for achievement in science in 2000 and the Navy Meritorious Civilian Service Award in 1991. He was a corecipient of the award for the best unclassified paper at the IEEE Military Communications Conference in 1995.